Chapter 26: System Roles & Permissions

System permissions are used in SEER*DMS to control access to specific functions or data. Roles are sets of system permissions. SEER*DMS allows registry managers to create roles as described in this chapter and to assign one or more roles to each user account (see *Chapter 25: Managing User Accounts)*.

In this chapter, you'll learn about

- Understanding System Roles and Permissions
- Using the Role Manager
- Creating a New Role
- Modifying a Role
- Printing a Role's Permissions
- Printing or Viewing a Role's User List
- Deleting a Role

Understanding System Roles and Permissions

The table below lists all system permissions in SEER*DMS. The permissions restrict access at three levels:

1. A permission may control access to a full menu or to individual items on a menu. If a user does not have the necessary permission, the menu or menu item will not be visible. For example, users who do not have the *fb_manager* permission will not see Follow-back on the Manage menu.

2. A permission may determine if a user can view or open a specific type of task. For example, users who do not have the *consolidate* permission will not see Consolidate tasks in the worklist, or in the worklist summary on the home page. Consolidate tasks cannot be assigned or re-routed to them.

3. A permission may restrict access to specific buttons or links on a page. For example, users who have the *rec_edit* permission will be able to perform Resolve Record Errors tasks. But, unless their role also includes the *fb_initiate* permission, they will not be able to submit follow-back needs while performing the tasks.

A set of permissions may be required to perform an operation. Consider the *consolidation* of patient data as an example. If a user has the *consolidate* and *pat_edit* permissions, they will be able to open consolidate tasks and make changes to the patient set data fields as they consolidate. However, they are likely to require other permissions, such as *fb_initiate*, to complete the task.

Permission	**A user with this permission has the ability to:**	**For more information see:**
afl_initiate	Create an Abstract Facility Lead (AFL)	Chapter 21: Managing Abstracting Assignments
afl_manager	Assign, track, and update AFLs	
afup_manager	Modify, track, and update active follow-up (AFUP) needs	Chapter 16: Follow-up
afup_modify	Modify an AFUP need	
consolidate	Open Consolidate tasks (pat_edit is required to consolidate the data)	Chapter 12: Consolidating Data

consolidate_fup	Open Consolidate FUP tasks (pat_edit_demographics or pat_edit is required to consolidate the data)	Chapter 16: Follow-up
contact_add	Add a physician, organization representative, or other contact	Chapter 19: The Contact List
contact_delete	Delete a contact (not implemented in the current version of SEER*DMS)	
contact_edit	Edit information for a physician, organization representative, or other contact	
contact_view	View Contact List in read-only mode	
extract_create	Create a data file by executing one of the standard extracts in the reports and extracts manager (View > Reports)	Chapter 24: Creating Reports and Extracting Data
facility_add	Add a new facility	Chapter 18: The Organization and Facility List
facility_delete	Delete a facility (not implemented in the current version of SEER*DMS)	
facility_edit	Edit a facility	
facility_view	View Organization and Facility List in read-only mode	
fb_initiate	Add a follow-back need (through the record or patient set editor)	Chapter 22: Follow-back
fb_manager	Modify, re-assign, or re-query follow-back needs; send follow-back queries and process responses	
import_electronic	Load data files through the SEER*DMS interface	Chapter 5: Importing Data Files
import_manual	Perform data entry	Chapter 6: Data Entry
import_resolution	Open Import Problems tasks	Chapter 5: Importing Data Files
lkup_modify	Add or edit codes to lookup lists (the lookups affected differ by registry)	
match	Select or reject matches in Match-Consolidate tasks	Chapter 10: Matching Incoming Records to Database
news_add	Add a news item. You may edit and delete items that you add.	Chapter 3: Using SEER*DMS
news_delete	Delete a news item entered by another user.	
news_edit	Edit a news item entered by another user.	
pat_delete	Delete a Patient, CTC, TX, or TXr (pat_edit is also required)	Chapter 11: The Patient Set Editor
pat_edit	Modify patient set fields other than over-ride flags, perform census tract resolution, use Patient Lookup, open Visual Edit Patient Set tasks	
pat_edit_demographics	Modify fields on demographic and comment pages of a patient set, use Patient Lookup	
pat_edit_overrides	Modify the over-ride flags in a patient set (pat_edit is also required)	
pat_end_task	Forward Resolve Patient Errors task to next workflow task regardless of the number of errors; does not affect submissibility (CTC status)	
pat_lookup_advanced	Use an alternate search algorithm in the Patient Lookup (if more than one algorithm is defined)	Chapter 20: Searching for Records and Patients

pat_read_only	Access a patient set in read-only mode, use Patient Lookup	Chapter 11: The Patient Set Editor
pat_undelete	Undelete a Patient, CTC, TX or TXr (pat_edit is also required)	
rec_build_cfo	Build a CTC from a casefinding record while editing the record	Chapter 21: Managing Abstracting Assignments
rec_build_dco	Build a CTC from a death certificate record while editing the record	Chapter 17: Death Clearance
rec_build_sho	Build a CTC from a short health record while editing the record	
rec_edit	Modify a record; use Patient Lookup	Chapter 8: Resolving Record Errors
rec_read_only	Access a record in read-only mode; use Patient Lookup	Chapter 20: Searching for Records and Patients
record_request_add	Create and send requests to outside organizations for records; view list of current Record Requests	Chapter 23: Requesting Records
record_request_resolve	Send, track, or update record requests in Record Request Manager	
reports	Access and generate standard reports	Chapter 24: Creating Reports and Extracting Data
reports_management	Access and generate management reports	
res_pat_errors	Open Resolve Patient Set Errors tasks (pat_edit is also required to complete the task)	Chapter 14: Resolving Patient Set Errors
res_rec_errors	Open Resolve Record Errors tasks (rec_edit also required to complete task)	Chapter 8: Resolving Record Errors
role_add	Add a new system role	Chapter 26: System Roles & Permissions
role_delete	Delete a system role (role_edit permission is also required)	
role_edit	Edit a system role	
screening	Set reportability status of a record	Chapter 9: Screening for Reportability
study_add	Add a special study	Chapter 28: Special Studies
study_delete	Delete a special study	
study_edit	Edit a special study	
study_pat_edit	Add or remove a patient set from a special study	
study_rec_edit	Add or remove a record from a special study	
system_administration	Provides control of system processes: execute system administration tasks (System > Tasks); terminate tasks regardless of task assignment	Chapter 28: System Administration
system_errors	View and manage System Error tasks	Chapter 28: System Administration
user_add	Add a new user account	Chapter 25: Managing User Accounts
user_delete	Delete a user account (user_edit is also required)	
user_edit	Edit a user account	
view_management_tasks	Access the Tasks section of the System menu; execute system tasks that do not require the system_admin permission	Chapter 28: System Administration
vis_edit_pat	Open Visual Edit Patient Set tasks (pat_edit also required to edit)	Chapter 13: Visual Editing

worklist_task_reassignment	Re-route or release worklist tasks	Chapter 4: Using the Worklist
worklist_task_terminate	End a task without forwarding the record or patient set to subsequent tasks in the workflow. You can only terminate tasks assigned to you; and unassigned tasks that you have permission to access.	

Using the Role Manager

Requires system permission: *role_add, role_edit,* or *role_delete*

The system roles available in SEER*DMS are defined by registry management and vary from registry to registry.

*To view the list of SEER*DMS roles defined for your registry:*

1. Select **System** > **Roles**
2. To sort the list by the data in a column, click on the linked (underlined) column heading.
3. To print the permissions associated with a role, click the **report** link.

The **Last Editor** column shows the user who last edited and saved the role. The **Last Edited** column shows the date and time stamp when it was last saved.

The function of the **copy** link is described in *Creating a New Role*. The **edit** link is described in the *Modifying a Role* section of this chapter.

Creating a New Role

Requires system permission: *role_add*

*To create a new role in SEER*DMS:*

1. Select **System** > **Roles**
2. There are two mechanisms for creating a new system role in SEER*DMS:
   a. To create a role by using an existing role as a template, click the **copy** link adjacent to an existing role. Use this technique if you are creating a role with a similar set of permissions as an existing role.
   b. To create a role using a blank template, click **Add**.
3. Enter a **Role Name** consisting of 2-30 alphanumeric characters. Role names must be unique.
4. Enter the text in the **Description** field. This description will be displayed in the Role Manager and in reports.
5. Check **Allow** for each system permission that is appropriate for this role.
6. Click **Save** to create and save the new role.

The new role will have no impact until the role is assigned to user accounts (instructions are provided in *Chapter 25: Managing User Accounts* chapter).

Modifying a Role

Requires system permission: *role_edit*

To make changes to the name, description, or permissions assigned to a role:

1. Select **System** > **Roles**
2. Click the role's name or its adjacent **edit** link.
3. Make any necessary modifications to the role's **Name** or **Description**. SEER*DMS uses underlying role IDs to manage the assignments of users to roles. Therefore, changing the name of the role does not affect the accounts of any users. Users that had this role with its old name will continue to have the role with the new name.
4. Check **Allow** for each system permission that is appropriate for this role. Uncheck any permission that is not appropriate.
5. Click **Save** to save your revisions. Changes to the role's permission settings will not affect a user's current session. The changes will go into affect the next time the user logs into SEER*DMS.

Printing a Role's Permissions

Requires system permission: *role_add, role_edit,* or *role_delete*

To create a report showing the permission settings for a role:

1. Select **System** > **Roles**.
2. Click the **report** link for the role of interest. The report engine will generate a system report in PDF.
3. Depending on your browser settings, you may have the option to Open or Save the report. If so, click Open. The PDF will open in an Adobe Acrobat window.
4. The report includes a list of the system permissions activated for this role. The report titles include the role name, description, date last modified, and the user name of the person who last modified this role.
5. Use the Adobe controls to print or save this report.
6. Close the Adobe window.

Printing or Viewing a Role's User List

Requires system permission: *role_edit*

To print or view the users who have a specific role:

1. Select **System** > **Roles**.
2. Click the role's name or its adjacent **edit** link.
3. Click **View Users (n)**, where n = number of active user accounts with this role. The report engine will generate a system report in PDF.
4. Depending on your browser settings, you may have the option to Open or Save the report. Click Open. The PDF will open in an Adobe Acrobat window.

5. The report lists the name and user name for the user accounts which are active and have this role. The “Other Roles” column indicates if this is the user’s only role.

6. Use the Adobe controls to print or save this report as necessary for maintaining the user accounts.

7. Close the Adobe window.

Deleting a Role

Requires system permission: *role_delete* and *role_edit*

Caution: Users are assigned system permissions via the role or roles that are assigned to their user accounts. Typically, each user account will have only one role. If you delete a user’s only role then you will be removing all system permissions for that user. They will be able to log in and use some functions in the View menu; all other system functions will be disabled for their account.

*To delete a system role in SEER*DMS:*

1. Select **System** > **Roles**

2. Click the role’s name or its adjacent **edit** link.

3. Click **View Users** to generate a report of the user accounts that currently have this role. This report includes a column labeled “Other Roles”. Print or save this report so that you can assign alternate roles to users with an “N” in this column.

4. Click **Delete**.

5. Click **OK** to confirm the deletion.